

TITLE OF INVENTION

FORWARD-SECURE COMMERCIAL KEY ESCROW SYSTEMS  
AND ESCROWING METHODS THEREOF

FIELD OF THE INVENTION

5  
10  
15  
The present invention relates generally to the cryptosystems and more particularly to a forward-secure commercial key escrow system that is interoperable with the PKI (Public Key Infrastructure) environment. More specifically, the present invention relates to a forward-secure commercial key escrow system that enables a given entity to monitor communications of users suspected of unlawful activities while protecting the privacy of law-abiding users.

DESCRIPTION OF THE RELATED ART

20  
25  
A rapid growth of digital communication over internet have resulted in the development of information technology, Network security and particularly cryptographic technology. Cryptographic technology is widely used to ensure the privacy and authentication of messages communicated over insecure channels such as internet.

Cryptography can be used to protect the

confidentiality of information by limiting access to the plain text data.

It has many advantages of using cryptography in electronic commerce and contracts over the internet for privacy and user authentication. But, the following problems may arise from the encryption key management.

First of all, a genuine user himself might not be able to access his information due to the loss or the damage of the decryption key.

Secondly, from the aspect of a company, there is a latent threat that can be caused by the misuse of the cryptosystem. For example, a rogue employee may encrypt the critical information of a company and then request money for releasing the decryption key.

Finally, from the aspect of a government, it sometimes happens that the government needs to have the right of an access to a key or plaintext with legal reasons such as the criminal investigation. Actually, the suspect can disturb the legal investigation by encrypting the information that has a relation to the crime.

The problems of the user's aspect can be solved if a commercial KES that provides services such as key-backup is used.

Furthermore, the second issue from the

aspect of a company or a government can be solved if a mandatory KES is employed as a security policy.

Many countermeasures such as lawful  
restriction for the usage of a cryptosystem with  
a hidden trapdoor have been studied to prevent  
the cryptographic side effects. Among them the  
KES is a typical solution.

In general, the key escrow system can be  
defined as a cryptosystem that allows an  
authorized person to retrieve the decryption key  
under the pre-determined condition.

Here, the predetermined condition means  
user's request for the description key when a  
desirable KES (Key Escrow System) satisfy the  
opposite features between protecting user's  
privacy and guaranteeing law enforcement. But  
practically, it is not an easy task to fulfill  
these requirements at the same time.

As a prior art in the field of the key  
escrow system for the PKI environment, the KES  
technologies from Netscape, VeriSign, and  
Entrust have been disclosed. They are very  
popular PKI-based key escrow system. The  
detailed descriptions of the above-mentioned  
company's KES technology will be provided in the  
following in order to understand the  
shortcomings of the prior art.

First of all, let us summarize the meaning of the terminology used in the conventional KES. The user is defined as an entity using PKI-based commercial key escrow system. The registration authority, which is abbreviated as RA, is a server that registers or vouch for the identity of users to a CA that then issues certificates.

The certification authority, which is called as CA in short, is a server that manages certificates for encryption and authentication.

The key management agent (KMA), is a trusted server coordinating the key recovery agents (KRA). The KRA is a server or an administrator to provide a key recovery information to a KMA.

FIG.1A is a schematic diagram illustrating the workflow of the Netscape's certificate management system (CMS) for a commercial key escrow system as a prior art. The detailed description of the Netscape's CMS can be found in the Netscape certificate management system administrator's guide version 4.1 ([http://docs.iplanet.com/docs/manuals/cms/41/adm\\_guide/contents.html](http://docs.iplanet.com/docs/manuals/cms/41/adm_guide/contents.html)).

Referring to FIG.1A, the user generates an encryption key pair  $(S_A, P_A)$ . Further, the user encrypts a private key  $(S_A)$

with the public key ( $P_{KMA}$ ) of the KMA, which is called as data recovery manager by Netscape, and sends the encrypted key  $E_{P_{KMA}}(S_A)$  as well as the user's public key ( $P_A$ ) to the RA 11 (step S100).

Thereafter, the RA forwards the user's encrypted key  $E_{P_{KMA}}(S_A)$  together with the user's public key ( $P_A$ ) to the KMA 13 for requesting the key escrow (step S101).

Now, the KMA 13 decrypts the encrypted key  $E_{P_{KMA}}(S_A)$  with the KMA's private transport key ( $S_{KMA}$ ), and checks that the user's private key ( $S_A$ ) corresponds to the user's public key  $P_A$ .

Then the KMA encrypts the user's private key  $S_A$  with the KMA's storage key ( $P'_{KMA}$ ) and stores the encrypted key in its internal database 17 (step S102).

Once user's private key has been successfully stored, the KMA digitally signs a token confirming that the key has been successfully stored.

The KMA's private key for storage is reserved in a software or hardware token and is protected by a PIN code.

The KMA 13 splits the PIN into  $n$  pieces with  $(m, n)$ -secret sharing scheme and then stores them encrypted with the passwords of  $n$  KRAs 14, 15, 17, respectively.

Referring to FIG.1A again, the KMA 13

sends a digitally signed token with the KMA's private transport key to the RA 11. The signed token means that the escrow of the user's private key ( $S_A$ ) has been successfully completed (step S104).

Thereafter, the RA 11 verifies the signed token and sends the certificate request to the CA 12 (step S105). The CA 12 issues and returns the encryption certificate to RA 11 (step S106), which is forwarded to the user 10 (step S107).

FIG.1B is a schematic diagram illustrating the key recovery process from the Netscape's CMS. Referring to FIG.1B, when the user 10 requests that KMA recover his or her private key, KMA subjects the request to its policy checks (step S120).

If the request passes all the policy rules, the KMA 13 sends a confirmation messages to n KRAs 14, 16 (step S121).

After verifying the confirmation, the KRAs then send their individual identifiers and passwords  $PSWD_1, PSWD_2, \dots, PSWD_n$  to the KMA 13 (step S122). After the verification process of checking if the required number of KRAs send their passwords, the KMA constructs the PIN for accessing the private key repository with the passwords of KRAs.

The KMA 13 retrieves the user's encrypted private key from its key repository and decrypts it with the private component of the storage key pair. Finally, the KMA securely sends the recovered private key to the user 10 (step S123).

FIG.2A is a schematic diagram illustrating the key escrow process of the VeriSign's Key Management Service product. More detailed information can be referred in a document "Onsite key management service administrator's guide (<http://www.verisign.com>)".

The feature of the VeriSign's key escrow system is that both the private key and the KMA 13 generate user's encryption key pair, which is called a key manager in the literature.

Referring to FIG.2A, once the user 10 requests the certificate for encryption (step S130), the RA 11 forwards the request to the KMA 13 (step S131). The KMA 13 generates an encryption key pair as well as a unique triple DES key for the user.

Thereafter, the KRR (Key Recovery Record) and the KRB (Key Recovery Block) are constructed as follows.

Preferably, the KRR is constructed from the relation  $KRR = E_k(PRI)$ , and the KRB from the relation  $KRB = E_{P_{KRA}}(K)$  where  $k$  is a triple DES

Key, and PRI is the private key of the user while  $P_{KRA}$  is the public key of the KRA 14. A KRB is the symmetric key encrypted using KRA's public key(triple DES key).

5           Additionally, the KMA 13 stores the created KRR and KRB in the database 17 together with the user's identifier and then the triple DES key is destroyed. Moreover, the KMA 13 sends the certificate request of the user to the  
10 CA 12 (step S133).

          Consequently, the CA 12 sends the encryption certificate to the KMA 13 (step S134). Thereafter, the KMA 13 sends the private key for encryption and the certificate to the user 10  
15 securely(step S135). Then, the KMA 13 destroys the private key of the user.

          FIG.2B is a schematic diagram illustrating the key recovery process of VeriSign's KMS product. Referring to FIG.2B,  
20 when the user 10 requests that the KMA 13 recover his or her private key, the KMA 13 retrieves the KRB of the user from the database (step S141). Optionally, an organization may use two PINs (called "Emergency Recovery  
25 Codes" ), and thereby the level of security is enhanced from the requirement of the existence of a couple of KMA's administrators.

          The retrieved KRB and the request for



key recovery are transmitted to the KRA 14 (step S142). The KRA verifies if the KRB is valid and matches with two PINs. The KRA 14 then decrypts the KRB to recover the embedded triple-DES Key to decrypt the encrypted private key.

The KRA 14 returns the decrypted triple DES key to the KMA 12 (step S143). Thereafter, the KMA 13 decrypts the KRR (the encrypted private key) with the received triple DES key to recover the user's private key and then sends it to the user (step S144).

FIG.3A is a schematic diagram illustrating the key escrow system of Entrust Corporation. The Entrust's key escrow system (KES) is described at "Administering Entrust/PKI 5.0 on UNIX".

Referring to FIG.3A, the user sends a request for the encryption certificate to the RA 11 (step S150). The RA 11 then forwards the request to the CA 12 (step S151).

Now, the CA 12 generates the user's key pair upon the request. Furthermore, the CA 12 is responsible for the issuance of the encryption certificate.

The user 10's encryption key pair and the certificate are encrypted either with CAST-128 or with 3-DES, which are to be stored in the database 17 (step S152). In the meanwhile, the

CA 12 forwards the user's private key and certificate to the user 10 via the RA 11 (step S153, S154).

FIG.3B is a schematic diagram illustrating the key escrow process of Entrust's KES. Referring to FIG.3B, the user requests the key recovery to the RA 11 (step S160), and then the RA 11 forwards the request to the CA 12 (step S161).

The CA 12 retrieves the encrypted private key of the user from the database 17 and decrypts the user's encrypted private key (step S162).

For the recovery of the encrypted private key at the step of S162, the passwords of the operating managers are needed and the number of operating managers participating in the recovery process of the escrowed key can be suitably chosen in accordance with the security policy.

Finally, the CA 12 forwards the decrypted private key to the user through the RA (step S163, S164).

As far as the user's privacy is concerned, the traditional commercial key escrow system proposed by either VeriSign or Entrust, however, have shortcomings in common. Namely, the user's private key for encryption is

inevitably exposed to a third party at the initial step of generating a key in accordance with the prior art.

This is because anyone among the group of the user, the KMA, and the CA is capable of generating the user's key pair (including user's private key) according to the prior art.

Additionally, traditional KES (key escrow system) disclosed by VeriSign and/or Entrust is not practically applicable because the user's private key is not securely managed. For instance, the security of the user's private key relies on the KMA and/or the CA in case when either the KMA or the CA generates the user's private key.

Additionally, the KES disclosed by Netscape Corporation still has the similar problem because the KMA encrypts the user's private key with the KMA's transport key in order to verify the correspondence between the escrowed private key and the public key, which means that the user's private key is inevitably exposed to the KMA that is a third party.

Furthermore, the user's escrowed private key is encrypted with the key of the central server (for instance, the storage key of the KMA for Netscape, and CAST-128 or 3-DES key of the CA for Entrust) and stored in the database.

Even in the case of compromising the central server's long-term private key, there still exists a problem such as the reduction of the security of the user's escrowed private key.

Since KMA as a central server employs the CRS (Certificate Request Syntax) protocol in an effort to securely transmit the decrypted 3-DES key from KRM, KMA has overhead for using the CRS protocol.

In addition, the traditional commercial key escrow system still has the problem in a sense that the database is vulnerable to the concentrated attack. This is because the key is kept in a single database despite the fault tolerance due to the periodic back-ups.

#### SUMMARY OF THE INVENTION

In view of the above-mentioned problems, there is a need in the art for a key escrow system, which is not subject to these limitations.

Accordingly, it is an object of the present invention to provide a practical key escrow system that is interoperable with PKI (Public Key Infrastructure).

It is another object of the present invention to provide a key escrow system

supporting a PKI-roaming service in addition to the key-backup service. Here, a PKI-roaming service means that the user moving in the wireless Internet environments is able to enjoy mobile PKI-service through downloading the private key with password, which is entered anywhere at client terminal.

It is still another object of the present invention to provide a key escrow system supporting a lawful access to the user's private key. In other words, it is an object of the present invention provide a key escrow system that does not allow a third party such as the KMA or the KRA, for instance, to have an access to the user's private key for encryption without the lawful permissions like the user's recovery request or the order from the court.

Yet it is another object of the present invention to present a key escrow system that provides the perfect forward secrecy and the practical utility. Here, a server with perfect forward secrecy implies the one that does not reduce the security of the user's escrowed key despite making compromise with its long-term private key.

Practically, the server's feature of the perfect forward secrecy is a very important factor because much more information regarding

the encryption key is concentrated on the central managing server.

It is also another object of the present invention to present a key escrow system that provides the blindness of the KMA or the KRA, which means that the user's private key for encryption is invisible either to the KMA or to the KRA during the key recovery process.

It is still another object of the present invention to provide the key escrow system with the fault-tolerant database of the KMA.

It is further another object of the present invention to provide a key escrow system that is possibly implemented in software. The aspect of implementation in software is important because the commercial key escrow system has to be economical even with high quality. Thus software implementation would be better for further use in e-commerce.

In general, a high-performance key escrow system is built with a hardware providing a tamperproof. However, the present invention has a feature in a sense that the escrow system is implemented in software in order to satisfy the requirement both for the cost and for the utility in electronic commerce.

Yet it is another object of the present

invention to present a key escrow system providing a privacy of the user even in the case when applicable to mandatory KES. In other words, the present invention insures the user's privacy as much as possible.

It is further another object of the present invention to present a key escrow system that enhances the credibility of the user and prevents the possible attack to a single KRA. The present invention provides a new system with a feature that authorization to the key recovery should be distributed over several servers.

Yet another object of the present invention is to provide a key escrow system preventing the large-scale wiretapping.

It is suggested as a solution to enable the legal individual to wiretap only the selected users, and to prohibit illegal massive wiretapping computationally. In accordance with a broad aspect of the present invention, provided is a software-based key escrow system for the PKI environment that is beneficial to both the user and the authority.

As a result, it becomes possible to protect the user's privacy even with the extendibility to the PKI-roaming service and the practical utility in the commercial electronic applications.

BRIEF DESCRIPTION OF THE DRAWINGS

Further features of the present invention will become apparent from a description of the fabrication process in conjunction with the accompanying drawings of the preferred embodiment of the invention, which, however, should not be taken to be limitative to the invention, but are for explanation and understanding only.

In the drawings:

FIG.1A is a schematic diagram illustrating the key escrow process of the Netscape Corporation as a prior art.

FIG.1B is a schematic diagram illustrating the key recovery process of the Netscape Corporation as a prior art.

FIG.2A is a schematic diagram illustrating the key escrow process of VeriSign Corporation as a prior art.

FIG.2B is a schematic diagram illustrating the key recovery process of Verisign Corporation as a prior art.

FIG.3A is a schematic diagram illustrating the key escrow process of Entrust Corporation as a prior art.

FIG.3B is a schematic diagram illustrating the key recovery process of Entrust Corporation as a prior art.



FIG.4A is a schematic diagram illustrating the key escrow process of a first embodiment in accordance with the present invention, an RSA  $(n, n)$ -commercial KES.

FIG.4B is a schematic diagram illustrating the key recovery process of a first embodiment in accordance with the present invention, an RSA  $(n, n)$ -commercial KES.

FIG.5 is a schematic diagram illustrating the key escrow and recovery processes of a second embodiment in accordance with the present invention, an RSA  $(n, n)$ -mandatory KES.

FIG.6 is a schematic diagram illustrating the key escrow and recovery processes of a third embodiment in accordance with the present invention, an RSA  $(n, n)$ -mandatory KES.

FIG.7A is a schematic diagram illustrating the key escrow process of a fourth embodiment in accordance with the present invention, a Diffie-Hellman  $(n, n)$ -commercial KES.

FIG.7B is a schematic diagram illustrating the key recovery process of fourth embodiment in accordance with the present invention, a Diffie-Hellman  $(n, n)$ -commercial KES.

FIG.8 is a schematic diagram illustrating the key escrow and recovery process of a fifth embodiment in accordance with the present invention, a Diffie-Hellman (n, n)-mandatory KES.

FIG.9 is a schematic diagram illustrating the key escrow and recovery processes of a sixth embodiment in accordance with the present invention, a Diffie-Hellman (n, n)-mandatory KES.

FIG.10A and FIG.10B are a schematic diagram illustrating the key escrow and recovery processes of a seventh embodiment in accordance with the present invention, a Diffie-Hellman (t, n)-commercial KES.

FIG.11 is a schematic diagram illustrating the key escrow and recovery processes of an eighth embodiment in accordance with the present invention, a Diffie-Hellman (t, n)-mandatory KES.

FIG.12 is a schematic diagram illustrating the key escrow and recovery processes of a ninth embodiment in accordance with the present invention, a Diffie-Hellman (t, n)-mandatory KES.

#### DETAILED DESCRIPTION OF THE INVENTION

The present invention will be explained in detail with reference to the accompanying drawings.

Shown in FIG.4A and FIG.4B are the schematic representations of the key escrow and recovery process of a first embodiment in accordance with the present invention, an RSA (n, n)-commercial KES, respectively.

For the understanding of the features of the present invention, let us explain the notations used in the following context

- PWD: user's password, which is supposed to be memorized, for the PKI-roaming service
- VER: user's password verifier that is registered in the KMA.
- KRB: user's key recovery block.
- $(e_i, N_i)$  : the public key of the  $KRA_i$  for encryption ( $N_1 < N_2 < \dots < N_1 < \dots < N_n$ ).
- $d_i$ : the private key of the  $KRA_i$  for decryption.

Referring to FIG.4A, the user 10 generates a pair of private/public keys (PRI, PUB) for encryption. The KRB (key recovery block) is constructed by the user and then forwarded to the RA 11 along with the PUB (step S201).

The present invention has a feature that

the user himself encrypts PRI with PWD. In other words, the operation of  $C = E_{\text{PWD}}(\text{PRI})$  is performed by the user.

$$\text{KRB} = (\dots((C^{e_1} \bmod N_1)^{e_2} \bmod N_2) \dots)^{e_n} \bmod N_n \quad (1)$$

Referring to FIG.4A again, the RA 11 sends the KRB and PUB to the KMA 13 (step S202). In the meanwhile, the KMA divides the key recovery block into  $\ell$  shares ( $\text{KRB}_1, \text{KRB}_2, \dots, \text{KRB}_\ell$ ) with  $(m, \ell)$ -SS ( $m < \ell$ ) and stores each share with the user's identifier in the associate  $\ell$  databases 23 ( $\text{DB}_1, \text{DB}_2, \dots, \text{DB}_\ell$ ), correspondingly.

Preferably, the KRB is then destroyed as long as the divided shares are stored in each database in an appropriate manner. Thereafter, the KMA 13 sends the notice permitting the issuance of encryption certificate to the RA 11 (step S203).

The RA 11 then exhibits the permission for the issuance to the CA 12 and requests an encryption certificate for the public key of the user 10 (step S204).

Accordingly, the CA 12 issues encryption certificate (step S205) and sends it to the RA 11 (step S206). Further, the CA 12 opens an encryption certificate in the directory server

19. Finally, the RA 11 forwards the encryption certificate to the user 10 (step S207).

FIG.4B is a schematic diagram illustrating the key recovery process of a first embodiment in accordance with the present invention, an RSA  $(n, n)$ -commercial KES. Referring to FIG.4B, the user 10 sends a request for the recovery of the private key for encryption to the KMA 13 (step S210).

After completing the step of identifying the user 10, the KMA 13 retrieves  $m$  key recovery blocks  $(KRB_1, KRB_2, \dots, KRB_m)$  out of  $\ell$   $KRB_i$  and reconstructs  $KRB$  through the  $(m, \ell)$ -SS. As a preferred embodiment in accordance with the present invention, the encrypted private key  $E_{PWD}(PRI)$  is recovered by the KMA 13 through the following steps.

The KMA 13 randomly chooses a blind factor  $r$  ( $0 < r < N_1$ ) and calculates  $KRB'$  from the relationship of

$$KRB' = KRB \cdot (\dots ((r^{e_1} \bmod N_1)^{e_2} \bmod N_2) \dots)^{e_n} \bmod N_n.$$

Now, the KMA 13 sends the  $KRB'$  along with the request for the key recovery to the  $n$ -th key recovery server  $KRA_n$  (step S211). In a reverse order from the  $n$ -th  $KRA$  to the first  $KRA$  ( $KRA_n, KRA_{n-1}, \dots, KRA_1$ ), each  $KRA_i$  decrypts the received message with its own private key (step S212 through to S216).

$$KRA_n : KRB'_{(n)} = (KRB')^{d_n} \bmod N_n \quad (2)$$

$$KRA_{n-1} : KRB'_{(n-1)} = (KRB'_{(n)})^{d_{n-1}} \bmod N_{n-1} \quad (3)$$

.

.

.

$$KRA_2 : KRB'_{(2)} = (KRB'_{(3)})^{d_2} \bmod N_2 \quad (4)$$

$$\begin{aligned} KRA_1 : KRB'_{(1)} &= (KRB'_{(2)})^{d_1} \bmod N_1 \\ &= E_{PWD}(PRI) \cdot r \bmod N_1 \end{aligned} \quad (5)$$

The  $KRA_1$  sends the  $KRB'_{(1)} = E_{PWD}(PRI) \cdot r \bmod N_1$  to the KMA. Finally, the KMA 13 recovers  $C = E_{PWD}(PRI) = KRB'_{(1)} / r \bmod N_1$ .

More preferably, the KMA 13 that has the password verifier (VER) of the user 10 sends  $C = E_{PWD}(PRI)$  to the user in a secure fashion such as the password-based private key downloading protocol (step S217).

FIG.5 is a schematic representation illustrating the key escrow process of a second embodiment in accordance with the present invention, an RSA (n, n)-mandatory KES. For a mandatory KES of a second embodiment in accordance with the present invention, the RA has to check if the escrowed private key of the user for encryption has a correspondence to the public key of the user.

The second embodiment of the present invention discloses a technique that protects

the privacy of the user simultaneously with checking capability of the validity of the key recovery block from the user.

Referring to FIG.5, the user 10 generates a total of  $s$  passwords  $PWD_j$  ( $j=1, \dots, s$ ) and registers the  $s$  password verifiers  $VER_j$  corresponding to each password to the KMA 13 (step S221).

Now, the user generates  $s$  pairs of private/public keys for encryption ( $PRI_j, PUB_j$ ). In other words, the user 10 generates a set of  $s$  private keys ( $PRI_1, PRI_2, \dots, PRI_s$ ) and a set of  $s$  public keys ( $PUB_1, PUB_2, \dots, PUB_s$ ).

Thereafter the set of  $s$  private keys  $PRI_j$  is encrypted with a set of password  $PWD_j$  of the user ( $j= 1, \dots, s$ ).

In other words,  $C_j = E_{PWD_j}(PRI_j)$  ( $j = 1, \dots, s$ ) is calculated. In this case, the encrypting step with PWD can be skipped preferably during the process of constructing the KRB when applicable to the key escrow system for the urgent wiretapping.

Now, the user constructs  $s$  key recovery blocks with a relationship of

$KRB_j = (\dots((C_j^{e_1} \bmod N_1)^{e_2} \bmod N_2) \dots)^{e_n} \bmod N_n$  and sends

them along with the public keys  $PUB_j$  ( $j= 1, \dots, s$ ) to the RA 11 (step S222).

The RA 11 that has received the  $KRB_j$  ( $j = 1, \dots, s$ ) and  $PUB_j$  ( $j = 1, \dots, s$ ) sends a random number of  $k$   $1 \leq k \leq s$  to the user (step S223).

5 The user 10 opens  $(s-1)$   $KRB_j$  except  $KRB_k$  to RA 11. In other words, the password  $PWD_j$  and  $PRI_j$   $\forall j \neq k, 1 \leq k \leq s$  are sent to the RA 11 (step S224).

10 As a preferred embodiment in accordance with the present invention, the number  $s$  controls the strength of the security. More preferably, this scheme can be designed in such a way as a non-interactive KES with a hash function.

15 Further, the RA 11 that has received  $(s-1)$   $KRB_j$  except  $KRB_k$  examines the validity of  $PRI_j$  and  $PUB_j$  with the following equation.

$$KRB_j \stackrel{?}{=} (\dots (C_j^{e_1} \bmod N_1)^{e_2} \bmod N_2 \dots)^{e_n} \bmod N_n \quad (6)$$

where  $\forall j \neq k, 1 \leq j \leq s$ .

20 Once the validity of the one-to-one correspondence between the  $PRI_j$ ,  $PUB_j$ , and  $KRB_j$   $\forall j \neq k, 1 \leq j \leq s$  is checked, it is considered that it is still valid even when  $j = k$ . Then,  
25 the RA 11 sends the  $KRB = KRB_k$ , and  $PUB = PUB_k$  to the KMA 13 (step S225). The remaining steps S226 through to S230 are identical to the



processes of the first embodiment.

FIG.6 is a schematic diagram illustrating the key escrowing process of a third embodiment in accordance with the present invention, an RAS (n, n)-mandatory KES.

The third embodiment discloses a key escrow system wherein the private/public keys of the user are generated by the KMA 13, and encrypted with PWD of the user for transmitting to the user.

The third embodiment can be employed for the practical, safe, and robust key escrow system against shadow attack.

Referring to FIG.6, the user 10 sends a request for encryption certificate to the RA 11 (step S231). Then the request is forwarded to the KMA 13 (step S232) through the RA 11.

In the meanwhile, the KMA 13 constructs a pair of the user's private/public keys (PRI, PUB) for encryption. The KRB is constructed and stored in the database as illustrated in the following description.

First of all, the KMA 13 encrypts the user's private key PRI with password PWD. In other words, the operation of  $C = E_{\text{PWD}}(\text{PRI})$  is performed, followed by a step of destroying the PRI. Now, the KRB is calculated with the following equation.

$$KRB = (\dots((C^{e_1} \bmod N_1)^{e_2} \bmod N_2)\dots)^{e_n} \bmod N_n \quad (7)$$

Additionally, the KMA 13 divides the KRB into  $\ell$  shares with  $(m, \ell)$ -SS ( $m < \ell$ ) and stores each share  $(KRB_1, KRB_2, \dots, KRB_\ell)$  along with the user's identifier in the  $\ell$  databases,  $DB_1$  21,  $DB_2$  22,  $\dots$ ,  $DB_\ell$  23, respectively.

As a preferred embodiment, the KRB is destroyed, after storing  $KRB_1$  in the database. The KMA 13 sends the notice permitting the issuance of encryption certificate along with  $(C, PUB)$  to the RA 11 (step S233).

The RA 11 then presents the permission to the CA 12 for the issuance and requests a encryption certificate for the public key PUB of the user 10 for encryption (step S234).

Accordingly, the CA 12 issues the encryption certificate (step S235) and sends it to the RA 11 (step S236). Further, the CA 12 open an encryption certificate in the directory server 19.

Finally, the RA 11 forwards the certificate to the user 10 (step S237). The escrowed private key of the user in the mandatory KES can be recovered through the process illustrated in FIG.4B, and the KMA should mount a dictionary attack to recover the private key PRI of the user for encryption.

Now, let us review the features of the present invention with comparison to the prior art by referring to the following table.

Table 1. Comparison of features invention and prior art

		Netscape (Prior Art)	Verisign (Prior Art)	Entrust (Prior Art)	Invention
Commer cial KES	Lawful Access	Poor	Poor	Poor	Excellent
	Utility and Perfect forward secrecy	Poor	Poor	Poor	Excellent
	Blindness	Poor	Poor	Poor	Excellent
	Fault Tolerance of storage unit	Good	Good	Good	Excellent
	Feasibility with software	Excellent	Excellent	Excellent	Excellent
	Value-Added service	N/A	PKI- roaming service	PKI- roaming service	PKI- roaming service
Mandat ory KES	Division of authority for key recovery	Good	Good	Good(depen ding on Security Policy)	Excellent
	Large-scale wiretapping	Poor	Poor	Poor	Excellent

The present invention has a unique feature of lawful access because the private key of the user for encryption is encrypted with

password PWD that is privately kept only to the user and then encrypted with the KRA's public key in a successive manner for transmittance.

Moreover, since the second embodiment in accordance with the present invention, an RSA (n, n)-mandatory KES, preferably employs the cut & choose method for checking the validity of the escrowed private key of the user, a lawful access is guaranteed due to the fact that the secret KRB that has not been made open to a third party is sent to the KMA.

In the meanwhile, the prior art disclosed by VeriSign and Entrust corporations has a limitation in that the private key of the user can be exposed either to the KMA or to the CA during the generating and escrowing phase, not the recovering phase, because the KMA or the CA itself generates the private key of the user.

Furthermore, the prior art even from Netscape Corporation discloses a key escrow system wherein the private key of the user is encrypted with a key for transport of the KMA in order to examine the correspondence between the private key and the public key.

Therefore, it may happen that the private key of the user is exposed to the KMA during the generating and escrowing phase rather than the recovering phase.

Referring to the Table 1, the present invention has an overwhelming feature in terms of the utility and perfect forward secrecy. For instance, the prior art disclosed from Netscape and Entrust has a shortcoming in a sense that the escrowed key of the user is encrypted with the key of the server (i.e., DRM's storage key in Netscape and CA's CAST-128 key or triple DES key in Entrust) and once the private key of the server is made open to the public, the private key of the user for encryption will be in danger.

Moreover, the prior art disclosed from VeriSign Corporation still has a limitation because the key for the CRS protocol, which is employed for the encryption of the transmitted message, should kept in a secure fashion in order for the KMA to forward the decrypted 3-DES key to the KRA.

In the meanwhile, the present invention provides a technique that makes it possible to guarantee a perfect forward secrecy because it is not necessary for the KMA to administrate the extra private and public keys.

Moreover, it is not possible for the KMA to figure out the private key of the user either during the key generation and escrowing phase or during the key recovering phase since the private key of the user is encrypted with the

user's own password that the KMA doesn't know.

Furthermore, the blind decoding algorithm in accordance with the present invention does not allow any KRA to find out the information of the user's private key during the recovering step of the key.

The key escrow system in accordance with the present invention has further a feature of fault tolerance of the storage unit.

The periodic back-ups of the database in the prior art disclosed by Netscape, VeriSign, and Entrust still does not provide a fault tolerance since a single unit of database is vulnerable to the hacker's attack.

To the contrary, the KMA in accordance with the present invention divides the KRB into a number of shares and each piece of KRB is separately stored in the multiple units of database.

Therefore, it becomes possible to decrease the chance of being attacked by a hacker for the preferred embodiments in accordance with the present invention.

More preferably, the proactive secure algorithm allows the security of the KES in accordance with the present invention to be enhanced.

For the reader's reference, the

proactive secure algorithm can be referred in a paper titled "How to withstand mobile virus attacks," by R. Ostrovski and M. Young, pp.51-61, 10th ACM symposium proceeding, 1991.

5 In addition, the present invention has a feature of flexibility for implementation both in software and in hardware. The present invention also provides enough flexibility regardless of the platform when compared to the prior art like Clipper.

10 The technology for the Clipper is described in a paper titled with, "Escrow encryption Standard (EES)," FIPS PUB (federal information processing standards publication) published by NIST, 1994.

15 Referring to Table 1 again, the present invention has a feature of providing a PKI-roaming service due to the fact that the recovered key  $C = E_{PWD}(PRI)$  is supposed to be transmitted to the user in a secure manner through the password-based private key downloading protocol.

20 Additionally, the key escrow system in accordance with the present invention, unlike the prior art such as the VeriSign's system, prevents the KRA from abusing its authorized power since the authorization for the key recovery is shared by many KRAs.

Furthermore, the present invention has a feature of preventing a large-scale wiretapping since the KMA recovers the private key of the user through the dictionary attack as in the partial KES.

More preferably, the speed of the recovery process of the key can be enhanced through employing the technique disclosed in the U.S. patent application No. 76/193,977 (High-speed RSA public key cryptographic method).

In general, the sender and the receiver make an agreement on their session key by Diffie-Hellman key exchange protocol. Once the user's long-term private key is disclosed, all the communications are insecure.

Therefore, the limitation of the period of the wiretapping becomes an important issue for the recovery of the key.

One approach to resolve the above-mentioned problem is to employ a protocol of distributing the session key suggested by A.K. Lenstra. Detailed description about the protocol of distributing the session key can be found in a literature "A key escrow system with warrant bounds," pp. 197-207 of a book titled with "Advances in cryptology-crypto 95 published by Springer-Verlag, 1995".

Now, the followings are the description



about additional embodiments in accordance with the present invention, a Diffie-Hellman KES.

First of all, let us explain the notations used in the following context.

5           · PWD: the user's password for PKI-roaming service, which is supposed to be memorized.

          ·  $p$  : prime,  $P = qw + 1$ , where  $q$  is a large prime and  $w$  is a smooth composite.

10           ·  $g$  : a generator of  $G_q$ , where  $G_q$  is the unique subgroup of  $\mathbb{Z}_p^*$  of order  $q$ .

          ·  $(X_i, Y_i)$ : the  $KRA_i$ 's pair of encryption key, where  $y_i = g^{x_i} \bmod p$ .

15           FIG.7A is a schematic representation illustrating the generating and escrowing process of the key of a fourth embodiment in accordance with the present invention, a Diffie-Hellman  $(n, n)$ -commercial KES.

20           Referring to FIG.7A, the user 10 generates a pair of private/public keys (PRI, PUB) and transmits the KRB along with the PUB to the RA 11 (step S410).

25           Here, the user encrypts his private key PRI with his own password PWD. In other words, the user generates  $C$  with a relation of  $C = E_{\text{PWD}}(\text{PRI})$ .

          Thereafter, the user selects a random

number  $z$  from the range  $0 < z < q$ . Moreover, the KRB is constructed from the following equation.

$$KRB = (C_1, C_2) = (g^z \bmod P, C \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_n)^z \bmod P) \quad (8)$$

In the meanwhile, the RA 11 transmits the KRB and PUB to the KMA 13 (step S411). Additionally, the KMA divides the KRB into  $\ell$  share  $(KRB_1, KRB_2, \dots, KRB_\ell)$  with  $(m, \ell)$  - ss ( $m < \ell$ ) and stores each share with the user's identifier in each database ( $DB_1$  21,  $DB_2$  22,  $\dots$ ,  $DB_\ell$  23). After completing the storage, the KRB is destroyed.

The KMA 13 then sends the notice permitting the issuance of encryption certificate along with  $(C, PUB)$  to the RA 11 (step S412).

The RA 11 then presents the permission to the CA 12 for the issuance and requests a certificate for the user's public key PUB (step S413).

Accordingly, the CA 12 issues encryption certificate and open an encryption certificate in the directory server 19.

The CA 12 sends the certificate to the RA 11 (step S414). Finally, the RA 11 forwards the certificate to the user 10 (step S237).

FIG.7B is a schematic diagram illustrating the recovering process of the key of a fourth embodiment in accordance with the present invention, a Diffie-Hellman  $(n, n)$ -commercial KES.

Referring to FIG.7B, the user 10 sends a request for the recovery of the private key for encryption to the KMA 13 (step S550).

After completing the step of identifying the user 10, the KMA 13 retrieves  $m$  key recovery blocks  $(KRB_1, KRB_2, \dots, KRB_m)$  out of  $\ell$   $KRB_i$  and reconstructs the KRB through the  $(m, \ell)$ -SS ( $m < \ell$ ).

As a preferred embodiment in accordance with the present invention, the encrypted private key  $E_{PWD}(PRI)$  is recovered by the KMA 13 through the following steps.

The KMA 13 randomly chooses a blind factor  $r$  ( $0 < r < P-1$ ) and calculates  $C_1'$  from the relation of  $C_1' = C_1^r \bmod p$ .

Thereafter, the KMA 13 sends the calculated  $C_1'$  along with a request for the recovery of the private key to the key recovery agents  $(KRA_1, KRA_2, \dots, KRA_n)$ .

In addition, each  $KRA_i$  calculates  $C_1''_{(i)} = (C_1')^{x_i} \bmod P$  and then sends  $C_1''_{(i)}$  to the KMA 13 ( $i = 1, \dots, n$ ).

The KMA 13 recovers the key  $C = E_{PWD}(PRI)$

by calculating  $C_2 / (C_1^{(1)} \cdot C_1^{(2)} \cdot \dots \cdot C_1^{(n)})^{1/r} \bmod P$ .  
Finally, the KMA 13, which has a password  
verifier of the user 10, sends the recovered  
private key  $C = E_{\text{PWD}}(\text{PRI})$  to the user in a secure  
fashion such as the password-based private key  
downloading protocol.

FIG.8 is a schematic diagram  
illustrating the generating and escrowing  
process of a fifth embodiment in accordance with  
the present invention, a Diffie-Hellman  $(n, n)$ -  
mandatory KES.

For a mandatory KES of a fifth  
embodiment in accordance with the present  
invention, the RA performs an additional step of  
checking the validity of the escrowed KRB.

Referring to FIG.8, the user 10  
generates a total of  $s$  passwords  $\text{PWD}_j$  ( $j = 1, \dots, s$ ) and registers the  $s$  password verifiers  $\text{VER}_j$   
corresponding to each password to the KMA 13  
(step S510).

Now, the user generates a total of  $s$   
pairs of private/public keys for encryption  
( $\text{PRI}_j, \text{PUB}_j$ ). In other words, a set of  $s$  private  
keys ( $\text{PRI}_1, \text{PRI}_2, \dots, \text{PRI}_s$ ) and a set of  $s$  public  
keys ( $\text{PUB}_1, \text{PUB}_2, \dots, \text{PUB}_s$ ) are generated by the  
user 10.

Thereafter, a set of  $\text{KRB}_j$  ( $j = 1, \dots, s$ )  
is constructed and sent to the RA 11 along with

$PUB_j$  ( $j = 1, \dots, s$ ). The private key  $PRI_j$  is encrypted with the password  $PWD_j$  of the user himself 10. In other words,  $C_j = E_{PWD_j}(PRI_j)$  ( $j = 1, \dots, s$ ) is calculated.

5 Preferably, in the key escrow system that needs the urgent wiretapping, the encrypting step with  $PWD$  can be skipped during the generating step of the  $KRB$ . Additionally, a total of  $s$  random numbers  $z_i$  are chosen in a range of  $0 < z_i < q$  ( $j = 1, \dots, s$ ) and the  $KRB_j$  ( $j = 1, \dots, s$ ) is calculated from the following equation.

$$\begin{aligned} KRB_j &= (C_{1j}, C_{2j}) \\ &= (g^{z_j} \bmod P, C_j \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_n)^{z_j} \bmod P) \end{aligned} \quad (9)$$

15 In the meanwhile, the RA 11 chooses  $k$  randomly in a range of  $1 \leq k \leq s$  and sends  $k$  to the user (step S512). Preferably, the security level of the system can be varied with  $s$ .

20 Referring to FIG.8 again, the user 10 open  $(s-1)$   $KRB_j$  except the  $KRB_k$  to RA 11 (step S513). In other words, the password  $PWD_j$ ,  $PRI_j$  and  $z_j \quad \forall j \neq k, 1 \leq j \leq s$  are sent to the RA 11. Further, the RA 11, which has received  $(s-1)$   $KRB_s$  except the  $KRB_k$ , examines the validity and the correspondence of  $PRI_j$ ,  $PUB_j$ , and  $KRB_j$  with the following equation.

$$KRB_j \equiv (g^{z_j} \bmod P, C_j \cdot (Y_1 \cdot Y_2 \cdots Y_n)^{z_j} \bmod P) \quad (10)$$

As a preferred embodiment in accordance with the present invention, the number  $S$  controls the strength of the security. More preferably, this scheme can be designed in such a way as a non-interactive KES with a hash function. Now the RA 11 sends  $KRB = KRB_k$  and  $PUB = PUB_k$  to the KMA 13 (step S514). The remaining steps S515 through to S518 are identical to the processes of the fourth embodiment.

The Sixth embodiment can be employed for the practical, safe, and robust key escrow system against shadow attack.

FIG.9 is a schematic diagram illustrating the generating and escrowing process of a sixth embodiment in accordance with the present invention, a  $(n, n)$ -mandatory KES based on Diffie-Hellman.

Referring to FIG.9, the user 10 sends a request for an encryption certificate to the RA 11 (step S630). The RA 11 forwards the request to the KMA 13 (step S631). The KMA 13 generates a pair of private/public keys  $(PRI, PUB)$ , and constructs the KRB to store in a distributed database 21, 22, 23 (step S632).

The KMA 13 encrypts the user's private key PRI with user's password PWD. In other words,  $C = E_{\text{PWD}}(\text{PRI})$  is calculated. In this case, it is assumed that the password of the user 10 PWD has been pre-registered at the KMA 13.

Thereafter, a random number  $z$  is selected in the range of  $0 < z < q$ . The KRB is constructed from the following equation.

$$\begin{aligned} \text{KRB} &= (C_1, C_2) \\ &= (g^z \bmod P, C \cdot (y_1 \cdot y_2 \cdots y_n)^z \bmod P) \end{aligned} \quad (11)$$

Now, the KMA 13 divides the KRB into  $\ell$  shares  $(\text{KRB}_1, \text{KRB}_2, \dots, \text{KRB}_\ell)$  with  $(m, \ell)$ -SS ( $m < \ell$ ), and stores each share in the associated database  $(\text{DB}_1, \text{DB}_2, \dots, \text{DB}_\ell)$  of  $\ell$ , correspondingly, with the identifier of the user. After storing  $\text{KRB}_1$  in the database, the KRB is destroyed.

The KMA 13 then sends the permission to issue the encryption certificate along with  $(C, \text{PUB})$  to the RA 11 (step S633). The RA 11 then presents the permission to the CA 12 and requests a certificate for the public key of the user 10, PUB (step S634).

Accordingly, the CA 12 issues the certificate of encryption and makes it public at a directory server 19 (step S635). The CA 12

sends the certificate to the RA 11 (step S636).  
Finally, the RA 11 forwards the certificate to  
the user 10 (step S637).

For the fifth embodiment of this  
invention, the escrowed key can be recovered  
with the process depicted in FIG.7B. In this  
case, the KMA can recover the private key of the  
user, PRI, by mounting a dictionary attack on  
the password of the user.

For the sixth embodiment of the present  
invention, the escrowed key can also be  
recovered with the process in FIG.7B. In this  
case, the KMA can recover the private key of the  
user, PRI, by using the password available to  
the KMA.

Now, the following is a detailed  
description of another embodiment of this  
invention,  $(t, n)$ -commercial KES based on  
Diffie-Hellman ( $t < n$ ). The unique feature of  
the preferred Diffie-Hellman  $(t, n)$ -commercial  
embodiment in accordance with the present  
invention is that  $t$  KRAs out of  $n$  are enough for  
the recovery of the escrowed key.

- $x_i$  : a private key of  $KRA_i$  for  $1 \leq i \leq n$ .
- $y$  : a public key of the group of KRAs.
- $P$  : a prime,  $P = qw + 1$ , where  $q$  is a  
large prime and  $w$  is a smooth composite.
- $g$  : a generator of  $G_q$ , where  $G_q$  is the



unique subgroup of  $Z_p^*$  of order  $q$ .

Each  $KRA_i$   $i = 1, \dots, n$  chooses  $r_i \in_R Z_q$  and makes  $y_i = g^{r_i} \bmod P$  public. Each  $KRA_i$  selects a random polynomial  $f_i \in_R Z_q[x]$  of degree  $(t-1)$  such that  $f_i(0) = r_i$ . Let  $f_i(x) = r_i + a_{i,1} \cdot x + a_{i,2} \cdot x^2 + \dots + a_{i,t-1} \cdot x^{t-1} \bmod q$ , where  $a_{i,1}, a_{i,2}, \dots, a_{i,t-1} \in_R Z_q$ . Then the  $KRA_i$  computes  $f_i(j) \bmod q$   $\forall j \neq i, 1 \leq j \leq n$  and sends it to the  $KRA_j$  securely.

Thereafter, each  $KRA_i$  computes,  $g^{a_{i,1}} \bmod P, g^{a_{i,2}} \bmod P, \dots, g^{a_{i,t-1}} \bmod P$  and makes them public. Using received  $f_j(i)$   $\forall j \neq i, 1 \leq j \leq n$ , each  $KRA_i$  verifies if

$$g^{f_j(i)} \stackrel{?}{=} y_j \cdot (g^{a_{j,1}})^{i^1} \cdot \dots \cdot (g^{a_{j,t-1}})^{i^{t-1}} \bmod P \quad \forall j \neq i, 1 \leq j \leq n.$$

Let us define  $H$  as the set  $\{KRA_i | KRA_i \text{ is an honest KRA satisfying the previous step.}\}$

Each  $KRA_i$  computes its private key

$x_i = \sum_{j \in H} f_j(i)$  and keeps it secure. The KRAs compute and publish their group public key

$$Y = \prod_{j \in H} y_j.$$

FIG.10 is a schematic representation illustrating key generation, escrow process, and key recovery process of a seventh embodiment in accordance with the present invention, a  $(t, n)$ -commercial KES based on Diffie-Hellman.

Referring to FIG.10A, the user 10

generates a pair of private/public keys (PRI, PUB), and sends the KRB along with the PUB to the RA 11 (step S710). The user 10 encrypts his private key, PRI, with his own password, PWD.

Thereafter, a random number  $z$  in the range of  $0 < z < q$  is selected. In addition, the key recovery block is computed from the following equation.

$$\begin{aligned} \text{KRB} &= (C_1, C_2) \\ &= (g^z \bmod P, C \cdot y^z \bmod P) \end{aligned} \quad (12)$$

In the meanwhile, the RA 11 sends the key recovery block, KRB, and the public key, PUB, to the KMA 13 (step S711). The KMA 13 divides the KRB into  $\ell$  shares ( $\text{KRB}_1, \text{KRB}_2, \dots, \text{KRB}_\ell$ ) with  $(m, \ell)$ -SS ( $m < \ell$ ), and stores each share with user's identifier in each database ( $\text{DB}_1, \text{DB}_2, \dots, \text{DB}_\ell$ ).

After the completion of the storage, the KRB is destroyed. The KMA 13 then sends a permission to issue the certificate of the encryption (step S712). The RA 11 then presents the permission to the CA 12 and requests a certificate for user's public key, PUB (step S713).

Accordingly, the CA 12 issues the certificate of encryption and makes it public at

a directory server 19. The CA 12 sends the certificate to the RA 11 (step S714). Finally, the RA 11 forwards the certificate to the user 10 (step S715).

Referring to FIG.10B, the user 10 sends a request for the key recovery to the KMA 13 (step S850). After identifying the user 10, the KMA 13 retrieves  $m$  key recovery blocks ( $KRB_1, KRB_2, \dots, KRB_m$ ) out of  $\ell$  key recovery blocks and reconstructs the KRB through the  $(m, \ell)$ -SS ( $m < \ell$ ).

As a preferred embodiment in accordance with this invention, the encrypted private key  $E_{PWD}(PRI)$  can be recovered by the KMA 13 through the following steps. The KMA 13 randomly chooses a blind factor  $r$  ( $0 < r < P-1$ ) and calculates  $c_1'$  from the relation of  $C_1' = C_1^r \bmod P$ .

Thereafter, the KMA 13 sends the calculated  $C_1'$  along with a request for the key recovery to the key recovery agents ( $KRA_1, KRA_2, \dots, KRA_n$ ).

In addition, each of  $t$  key recovery agents calculates  $C_1''_{(i_j)} = (C_1')^{x_{i_j}} \bmod P$  and then sends  $(C_1''_{(i_j)}, i_j)$  to the KMA 13

$(1 \leq i_1 < \dots < i_j < \dots < i_t \leq n)$ . The KMA 13 receives  $t$   $(C_1''_{(i_1)}, i_1)$  pairs from the KRAs of  $t$ , and

recovers the encrypted private key  $C = E_{\text{PWD}}(\text{PRI})$

by calculating  $C_2 / \prod_1 (C_1^{r^{-1} \prod_{j=1}^{j/(j-1)}}) \bmod P$ .

Finally, the KMA 13, which has a password verifier of the user 10, sends the recovered  $c = E_{\text{PWD}}(\text{PRI})$  to the user in a secure fashion using "password-based private key downloading protocol".

Now, when we want to apply the  $(t, n)$ -commercial KES based on Diffie-Hellman to a mandatory KES having a protection against a large-scale wiretapping, the RA performs an additional step of checking the validity of the escrowed key recovery block.

In this case, cut & choose method as in the previous second embodiment can be preferably employed.

FIG.11 is a schematic diagram illustrating the key generation and escrow process of an eighth embodiment in accordance with this invention,  $(t, n)$ -mandatory KES based on Diffie-Hellman.

Referring to FIG.11, the user 10 generates a total of  $s$  passwords  $\text{PWD}_j$  ( $j = 1, \dots, s$ ) and registers the  $s$  password verifiers  $\text{VER}_j$  ( $j = 1, \dots, s$ ) corresponding to each password to the KMA 13 (step S910). Now, the user generates a total of  $s$  pairs of private/public keys for

encryption  $(PRI_j, PUB_j)$ .

Thereafter, a set of  $KRB_j$  ( $j = 1, \dots, s$ ) is constructed and sent to the RA 11 along with  $PUB_j$  ( $j = 1, \dots, s$ ).

The private key  $PRI_j$  is encrypted with the password  $PWD_j$  of the user 10. In other words,  $C_j = E_{PWD_j}(PRI_j)$  ( $j = 1, \dots, s$ ) is calculated. Preferably, in the key escrow system that needs the urgent wiretapping, the encrypting step with  $PWD$  can be skipped in the generating step of the  $KRB$ .

Additionally, a total of  $s$  random number  $z_j$  are chosen in the range of  $0 < z_j < q$  ( $j = 1, \dots, s$ ) and the  $KRB_j$  ( $j = 1, \dots, s$ ) is calculated from the following equation.

$$\begin{aligned} KRB_j &= (C_{1j}, C_{2j}) \\ &= (g^{z_j} \bmod P, C_j \cdot (y)^{z_j} \bmod P) \end{aligned} \quad (13)$$

In the meanwhile, the RA 11 randomly chooses  $k$  in the range of  $1 \leq k \leq s$  and sends  $k$  to the user (step S912). Preferably, the security level of this system depends on the size of  $s$ .

Referring to FIG.11 again, the user 10 opens  $(s-1)$   $KRB_j$  except the  $KRB_k$  to the RA 11 (step S913).

In other words, the  $PWD_j$ ,  $PRI_j$ , and  $z_j$  for  $\forall j \neq k$  and  $1 \leq j \leq s$  are sent to the RA 11. Further, the RA 11, which has received  $(s-1)$  key

recovery blocks except the  $KRB_k$ , examines the validity of the  $KRB_j$  and the correspondence of  $PRI_j$  and  $PUB_j$  for  $\forall j \neq k, 1 \leq j \leq s$ .

As a preferred embodiment in accordance with this invention, this scheme can be designed in such a way as a non-interactive one with a hash function.

Now the RA 11 sends  $KRB = KRB_k$  and  $PUB = PUB_k$  to the KMA 13 (step S914). The remaining steps S915 through to S919 are identical to the processes of the fourth embodiment.

As a preferred embodiment for robust and practical  $(n, n)$ -mandatory KES based on Diffie-Hellman that is secure against the shadow public key attack, a sixth embodiment is disclosed wherein the private/public key of the user is generated and encrypted by the KMA and then sent to the user.

FIG.12 is a schematic diagram illustrating the key generation and escrow process of a ninth embodiment in accordance with the present invention,  $(t, n)$ -mandatory KES based on Diffie-Hellman.

Referring to FIG.12, the user 10 sends a request for the certificate of encryption to the RA 11 (step S1210). Then the RA 11 forwards the request to the KMA 13 (step S1211).

The KMA generates a pair of

private/public keys (PRI, PUB) for the user, and constructs the KRB as illustrated in the following description.

The KMA 13 encrypts the private key of the user PRI with user's password PWD. In other words,  $C = E_{\text{PWD}}(\text{PRI})$  is calculated. In this case, it is assumed that the password of the user PWD has already been registered in the KMA 13. Thereafter, the KMA 13 selects a random number  $z$  in the range of  $0 < z < q$ .

Moreover, the KMA 13 constructs the KRB from the following equation.

$$\begin{aligned} \text{KRB} &= (C_1, C_2) \\ &= (g^z \bmod P, C \cdot y^z \bmod P) \end{aligned} \quad (14)$$

Additionally, the KMA divides the KRB into  $\ell$  shares  $(\text{KRB}_1, \text{KRB}_2, \dots, \text{KRB}_\ell)$  with  $(m, \ell)$ -SS ( $m < \ell$ ) and stores each share with user's identifier in each database ( $\text{DB}_1$  21,  $\text{DB}_2$  22,  $\dots$ ,  $\text{DB}_\ell$  23). After, completing the storage, the KRB is destroyed.

The KMA 13 then sends a permission to issue the certificate of encryption along with  $(C, \text{PUB})$  to the RA 11 (step S1212). The RA 11 then presents the permission to the CA 12 and requests a certificate for the public key of the user 10, PUB (step S1213).

Accordingly, the CA 12 issues the certificate of encryption and makes it public at a directory server 19. The CA 12 sends the certificate to the RA 11 (step S1214). Finally, the RA 11 forwards the certificate and C to the user 10 (step S1215).

For the eighth embodiment of this invention, the escrowed key can be recovered with the process illustrated in FIG.10B. More preferably, the private key of the user, PRI, can be recovered by mounting a dictionary attack on the password of the user.

For the ninth embodiment of this invention, the escrowed key can also be recovered with the process illustrated in FIG.10B. More preferably, the private key of the user, PRI, can be recovered with user's password that has been available with the KMA.

Although the present invention has been illustrated and described with respect to exemplary embodiments thereof, it should be understood by those skilled in the art that various other changes, omissions and additions may be made therein and thereto, without departing from the spirit and scope of the present invention.

It should be appreciated by those skilled in the art that the specific embodiments



disclosed above may be readily utilized as a basis for modifying or designing other techniques and processes for carrying out the same purposes of the present invention.

5 It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims.

10

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
22